LA GUERRE ELECTRONIQUE et L'INTELLIGENCE ARTIFICIELLE



Nicolae Sfetcu

MultiMedia Publishing

La guerre électronique et l'intelligence artificielle

APERÇU DU LIVRE

Nicolae SFETCU[1]

Publié par MultiMedia Publishing

Sfetcu, Nicolae (2024), *La guerre électronique et l'intelligence artificielle*, MultiMedia Publishing, ISBN 978-606-033-865-9, DOI : DOI: 10.58679/MM37958, https://www.telework.ro/fr/e-books/la-guerre-electronique-et-lintelligence-artificielle/

Publié par MultiMedia Publishing, https://www.telework.ro/fr/publication/

ISBN 978-606-033-865-9
DOI : DOI: 10.58679/MM37958
URL : https://www.telework.ro/fr/e-books/la-guerre-electronique-et-lintelligence-artificielle/

[1] Chercheur - Académie Roumaine - Comité Roumain pour l''Histoire et la Philosophie des Sciences et des Techniques (CRIFST), Division Histoire des Sciences (DIS), ORCID: 0000-0002-0162-9973

Table des matières

La guerre électronique et l'intelligence artificielle

Ing. Phys. Nicolae SFETCU, MPhil

Abstract

Electronic warfare is a critical component of modern military operations and has undergone significant advances in recent years. This book provides an overview of electronic warfare, its historical development, key components, and its role in contemporary conflict scenarios. It also discusses emerging trends and challenges in electronic warfare and its contemporary relevance in an era of advanced technology and cyber threats, emphasizing the need for continued research and development in this area.

The book explores the burgeoning intersection of artificial intelligence and electronic warfare, highlighting the evolving landscape of modern conflicts and the implications of integrating advanced technologies. The multifaceted roles of artificial intelligence in electronic warfare are highlighted, examining its potential advantages, ethical considerations, and challenges associated with its integration.

Keywords: electronic warfare, artificial intelligence, machine learning, cognitive warfare, asymmetric warfare, electromagnetic spectrum

Résumé

La guerre électronique est un élément essentiel des opérations militaires modernes et a connu des progrès significatifs ces dernières années. Ce livre donne un aperçu de la guerre électronique, de son évolution historique, de ses composants clés et de son rôle dans les scénarios de conflit contemporains. Il aborde également les tendances et les défis émergents en matière de guerre électronique et sa pertinence contemporaine à l'ère des technologies avancées et des cybermenaces, en soulignant la nécessité de poursuivre la recherche et le développement dans ce domaine.

Le livre explore l’intersection naissante de l’intelligence artificielle et de la guerre électronique, mettant en lumière l’évolution du paysage des conflits modernes et les implications de l’intégration des technologies avancées. Les rôles multiformes de l'intelligence artificielle dans la guerre électronique sont mis en évidence, en examinant ses avantages potentiels, les considérations éthiques et les défis associés à son intégration.

Mots-clés : guerre électronique, intelligence artificielle, apprentissage automatique, guerre cognitive, guerre asymétrique, spectre électromagnétique

Abréviations

AI = Artificial Intelligence (Intelligence artificielle, IA)
ANN = Artificial Neural Network (Réseau neuronal artificiel)
C&C = Command and Control (Commande et contrôle)
CDP = Capability Development Plan (Plan de développement des capacités)
CEW = Cybernetic Electronic Warfare (Guerre électronique cybernétique)
CNN = Convolutional Neural Network (Réseau neuronal convolutif)

CNO = Computer Network Operations (Opérations de réseau informatique)
COMINT = Communication Intelligence (Intelligence des communications)
CW = Cyber Warfare (Guerre cybernétique)
DE = Directed Energy (Énergie dirigée**)**
DL = Deep Learning (Apprentissage profond)
DNN = Deep Neural Network (Réseau neuronal profond)
DoD = US Department of Defense (Département de la Défense des États-Unis)
EA = Electronic Attack (Attaque électronique)
ECCM = Electronic Counter-countermeasures (Contre-contre-mesures électroniques)
ECM = Electronic Countermeasure (Contre-mesure électronique)
EDA = European Defence Agency (Agence Européenne de Défense)
ELINT = Electronic Intelligence (Intelligence électronique)
EM = Electromagnetic (Électromagnétique)
EME = Electromagnetic Environment (Environnement électromagnétique)
EMOE = Electromagnetic Operational Environment (Environnement opérationnel électromagnétique)
EMS = Electromagnetic Spectrum (Spectre électromagnétique)
EMSO = Electromagnetic Spectrum Operations (Opérations sur le spectre électromagnétique)
EOB = Electronic Order of Battle (Ordre de bataille électronique)
EP = Electronic Protection (Protection électronique)
EPM Electronic Protective Measures (Mesures de protection électroniques)
ES = Electronic Warfare Support (Support de guerre électronique)
ESM = Electronic Support Measures (Mesures de support électronique)
EW = Electronic Warfare (Guerre électronique, GE)
IoT = Internet of Thinngs (Internet des objets)
IO = Information Operation (Opération d'information, OI)
ISR = Intelligence, Surveillance and Reconnaissance (Renseignement, surveillance et reconnaissance)
JADC2 = US Joint All Domain Command and Control (Commandement et contrôle conjoints de tous les domaines des États-Unis)
JEMSO = Joint Electromagnetic Spectrum Operations (Opérations conjointes sur le spectre électromagnétique)
LAWS = Lethal Autonomous Weapon Systems (Systèmes d'armes autonomes létales)
MILDEC = Military Deception (Déception militaire)
ML - Machine Learning (Apprentissage automatique)
MLP = Multi-Layer Perceptron (Perceptron multicouche)
NDS = US National Defense Strategy (Stratégie de défense nationale des États-Unis)
OPSEC = Operations Security (Sécurité des opérations)
PSYOP = Psychological Operations (Opérations psychologiques)
RF = Radio Frequency (Fréquence radio)
SIGINT = Signal Intelligence (Renseignement sur les signaux)
UAV = Unmanned Aerial Vehicle (drone) (Véhicule aérien sans pilote (drone))

Relation de la guerre électronique avec d'autres capacités de combat

Guerre de l'information et cyber-guerre : À l'ère moderne, la guerre s'étend au cyberespace, où les agences de renseignement jouent un rôle essentiel dans la défense contre les cybermenaces. Ils surveillent activement les activités numériques, identifient les cyberattaques potentielles et évaluent les capacités des cyberacteurs hostiles. En outre, les services de renseignement se livrent à une guerre de l'information, contrecarrant la propagande ennemie et influençant l'opinion publique afin d'acquérir le pouvoir dans les conflits. L'un des défis majeurs de la guerre russo-ukrainienne a été le recours généralisé à des campagnes de désinformation de la part de la Russie et de l'Ukraine. La désinformation et la propagande ont été utilisées pour influencer l'opinion publique, manipuler les perceptions et semer la confusion dans les rangs ennemis. Les services de renseignement sont contraints de s'adapter et d'investir dans la lutte contre la désinformation, tout en garantissant la crédibilité et l'exactitude de leurs propres rapports. (Sfetcu 2023b)

La cyberguerre est une composante de la confrontation entre la Russie et l'Ukraine depuis l'effondrement de l'Union soviétique en 1991. Alors que les premières attaques contre les systèmes d'information des entreprises privées et des institutions publiques en Ukraine ont été enregistrées lors des manifestations de masse en En 2013, la cyber-arme russe Uroburos existe depuis 2005. La cyber-guerre russe s'est poursuivie avec la pénétration du réseau électrique ukrainien en 2015 à Noël, puis à nouveau en 2016 en paralysant le Trésor public ukrainien en décembre 2016 et une attaque informatique massive en juin 2017. et attaques contre les sites Web du gouvernement ukrainien en janvier 2022. (Sfetcu 2023b)

Guerre psychologique : Les activités de renseignement peuvent également jouer un rôle dans la guerre psychologique, où la diffusion d'informations soigneusement élaborées peut influencer le moral et la prise de décision de l'ennemi. En diffusant stratégiquement certaines informations ou désinformations, les services de renseignement peuvent créer de la confusion, de la méfiance et de l'incertitude parmi les forces opposées, sapant potentiellement leur détermination et leur cohésion. (Sfetcu 2023b)

Au siècle dernier, et surtout au cours de la seconde moitié, la guerre électronique a rejoint d'autres capacités de combat et est devenue l'une des compétences majeures de la guerre. Les cinq compétences de base réunies, PSYOP, CNO, EW, MILDEC et OPSEC, sont essentielles pour façonner l'environnement de l'information (Army 2020a, II-1).

Opérations de réseaux informatiques (CNO) et GE : plus la GE et la CNO sont intégrées, plus il est facile de collecter, de manipuler et de diffuser des informations, car le spectre EM est de plus en plus utilisé dans l'utilisation des réseaux informatiques, en particulier des réseaux sans fil.

Les États-Unis définissent une attaque de réseau informatique (CNA) comme incluant les opérations visant à perturber, nier, dégrader ou détruire les informations résidant dans les ordinateurs et les réseaux informatiques, ou dans les ordinateurs et les réseaux eux-mêmes (Army 2020a). Un réalignement de la terminologie, de la doctrine et même des systèmes du CNW, avec les leçons tirées de la guerre électronique, présente des avantages potentiels (R. Smith et Knight 2005).

Tromperie militaire (MILDEC) et guerre électronique : la tromperie militaire consiste en « des actions exécutées pour induire délibérément en erreur les décideurs militaires de l'adversaire quant aux capacités, intentions et opérations militaires amies, amenant ainsi l'adversaire à prendre des actions (ou inactions) spécifiques qui contribueront à l'accomplissement de la mission amicale » (Army 1996, I-1). Cette relation se développe à mesure que les militaires utilisent de plus en plus le spectre EM à des fins de tromperie.

Sécurité des opérations (OPSEC) et guerre électronique : la sécurité des opérations est le processus consistant à identifier des informations critiques et à les refuser aux décideurs adverses pour les amener à mal calculer les forces amies, les plans d'action et les intentions (Army 2020a, II-3). Les missions militaires qui peuvent éviter d'être détectées par les radars ennemis s'avèrent généralement plus efficaces. ES fourni à l'OPSEC des informations sur les capacités et les intentions de l'adversaire de collecter des renseignements sur les éléments essentiels du renseignement ami via le spectre EM. Dans une campagne militaire de déception, la déception électromagnétique et l'OPSEC doivent être intégrées, synchronisées et coordonnées.

Opérations psychologiques (PSYOP) et GE : Influencer l'adversaire doit toujours être l'objectif ultime des opérations d'information. Les progrès technologiques récents permettent à des capacités telles que PSYOP et MILDEC de fournir un plus grand nombre de capacités améliorées, nécessitant une plus grande implication de GE dans ces domaines. La guerre électronique facilite les opérations PSYOP en dégradant la capacité de l'ennemi à observer les activités sur le théâtre, à signaler ces activités et à prendre des décisions en conséquence (Kucukozyigit 2006).

Les compétences de soutien de l'OI sont la sécurité physique, l'attaque physique, le contre-espionnage (CI), l'assurance de l'information et la caméra de combat (COMCAM), qui contribuent directement ou indirectement à l'efficacité de l'OI.

Sécurité physique et guerre électronique : L'utilisation d'un dispositif de brouillage pour les convois militaires peut être considérée comme une sécurité physique. Des mesures de sécurité physique sont utilisées partout où des équipements de guerre électronique sont présents (Army 2020a, B-2).

Attaque physique et guerre électronique : L'attaque physique perturbe, détruit ou endommage des cibles de toute sorte en utilisant une puissance cinétique destructrice, fournissant un moyen efficace d'attaquer les systèmes de guerre électronique adverses et renforçant ainsi la supériorité des opérations de guerre électronique amies.

Contre-espionnage (CI) et guerre électronique : Le CI comprend les informations collectées et les activités menées pour contrer le renseignement, l'espionnage, le sabotage, l'assassinat, etc. de l'adversaire (Army 2020a, II-7). CI soutient l'EP et l'ES en fournissant des contre-mesures électroniques (Army 2020a, B-3), et les ressources de guerre électronique peuvent être utilisées pour détruire ou dégrader les capacités de renseignement de l'ennemi. Le renseignement électronique collecté grâce aux capacités SIGINT et ES est utilisé pour évaluer, analyser et mettre à jour les capacités de renseignement de l'ennemi.

Les mesures de contre-espionnage visent à empêcher les adversaires de s’infiltrer et de recueillir des informations sensibles auprès des forces amies. Ceci est essentiel pour maintenir la sécurité opérationnelle et garantir que les stratégies et tactiques de chacun restent confidentielles. Les services de renseignement surveillent la protection des informations sensibles et des opérations militaires contre toute compromission par des agents hostiles. L'identification et la neutralisation des espions ennemis peuvent avoir un impact significatif sur la capacité de l'ennemi à recueillir des renseignements et à perturber ses plans. La guerre russo-ukrainienne se caractérise par le recours généralisé de la Russie à la désinformation et aux tactiques de guerre hybride. Les services de renseignement jouent un rôle essentiel dans la détection et la lutte contre ces efforts. Ils surveillent les réseaux sociaux, les forums en ligne et les médias traditionnels pour identifier les faux récits et la propagande diffusée par des acteurs hostiles. De fausses informations sont utilisées pour provoquer l’indignation du public en temps de guerre. En avril 2014, les chaînes d’information russes *Russia-1* et *NTV* ont montré sur une chaîne un homme affirmant avoir été

attaqué par un gang fasciste ukrainien, et sur l'autre, affirmant qu'ils finançaient la formation de radicaux de droite anti-russes. En mai 2014, Russia-1 a diffusé un reportage sur les atrocités ukrainiennes à partir d'images d'une opération russe menée en 2012 dans le Caucase du Nord. Le même mois, le réseau d'information russe *Life* a présenté une photo de 2013 d'un enfant blessé en Syrie, victime des troupes ukrainiennes qui venaient de reprendre l'aéroport international de Donetsk. En comprenant le paysage de la désinformation, les services de renseignement peuvent informer les gouvernements et le public des tactiques trompeuses utilisées par la Russie, garantissant ainsi que la désinformation n'influence pas l'opinion publique ni ne compromet les autorités nationales (Sfetcu 2023b).

Caméra de combat (COMCAM) et guerre électronique : La COMCAM fournit aux dirigeants des images pour répondre aux exigences opérationnelles et de planification (Army 2020a, II-7). Les capacités ES de soutien au renseignement contribuent également à la mission de la COMCAM à travers le spectre des conflits. COMCAM peut être utilisé pour évaluer l'efficacité du ciblage de guerre électronique, et EP contribue à la mission COMCAM en transmettant en toute sécurité les images COMCAM.

Assurance de l'information (IA) et GE : L'IA comprend des mesures qui protègent et défendent les informations et les systèmes d'information. La guerre électronique offre une protection opérationnelle contre les efforts de l'adversaire et du renseignement ciblant les informations électroniques et les systèmes d'information amis(Army 2020a, II-6), et soutient l'IA en protégeant les informations, les systèmes d'information et les actifs (Army 2020a, B-3)

Guerre cyber-électronique

Au début des années 2000, la cyberguerre a commencé à émerger comme un nouveau concept. Ses atouts se sont confirmés lors de la seconde guerre du Golfe, en Estonie en 2007 lorsqu'elle a été exposée à une cyber-attaque russe (Dunn Cavelty 2012), et en Géorgie lors de la guerre d'Ossétie du Sud en 2008 (Yasar, Yasar, et Topcu 2012).

La cyberguerre implique le recours à des cyberattaques au niveau des États, causant des dégâts comparables à une guerre réelle et/ou perturbant les infrastructures et les systèmes ennemis (Singer et Friedman 2014).

Taddeo a proposé la définition suivante de la cyberguerre en 2012 :

« La [cyber] guerre est [la guerre fondée sur certaines] utilisations des TIC dans le cadre d'une stratégie militaire offensive ou défensive approuvée par un État et visant à la perturbation

> ou au contrôle immédiat des ressources de l'ennemi, et qui est menée dans l'environnement informationnel, avec agents et cibles allant à la fois dans les domaines physiques et non physiques et dont le niveau de violence peut varier selon les circonstances. » (Taddeo 2012)

La cybersécurité et la cyberguerre sont devenues des enjeux critiques dans un monde de plus en plus interconnecté. La cybersécurité (la pratique consistant à protéger les systèmes et les données numériques contre les activités malveillantes) est inextricablement liée à la cyberguerre, qui implique l'utilisation de technologies numériques pour perturber, endommager ou prendre le contrôle des systèmes informatiques adverses. La frontière entre ces deux domaines est floue, dans la mesure où les stratégies de cybersécurité ont souvent une double utilité en tant qu'applications dans la cyberguerre et vice versa.

La cybersécurité et la cyberguerre sont étroitement liées dans une relation complexe qui façonne notre monde numérique. Alors que les cybermenaces continuent d'évoluer et que les États-nations s'engagent dans des cyberactions offensives, la nécessité de mesures de cybersécurité robustes et d'une coopération internationale est plus cruciale que jamais. Pour naviguer efficacement dans ce lien complexe, les parties prenantes doivent continuellement s'adapter à la nature dynamique du domaine cybernétique, en reconnaissant que la guerre numérique est aussi importante que n'importe quel champ de bataille physique au 21e siècle.

À l'ère du numérique, le paysage des menaces évolue constamment, nécessitant des mesures de cybersécurité adaptatives. Les cybermenaces englobent un large éventail d'activités, notamment le vol de données, les attaques de logiciels malveillants, les attaques par déni de service et l'ingénierie sociale. Ces menaces peuvent cibler des individus, des organisations ou même des nations entières. À mesure que les cybermenaces deviennent de plus en plus complexes, le défi consistant à sécuriser les infrastructures critiques et les informations sensibles augmente également.

La relation entre cyberguerre et guerre électronique peut être considérée comme la relation entre guerre asymétrique et guerre symétrique. La cyberguerre et la guerre électronique ont été utilisées ensemble pour la première fois lors de la guerre entre la Russie et la Géorgie en 2008 (Yasar, Yasar, et Topcu 2012).

Alors que la guerre électronique utilise le spectre électromagnétique et que la CW utilise des éléments du cyberespace, la cyberguerre électronique propose l'intégration de ces deux capacités de combat. L'avantage du CEW est que même si une attaque électronique peut être détectée, une cyberattaque électronique est presque impossible à détecter.

Yasar, Yasar et Topcu effectuent une analyse SWOT de l'AI, concluant que même s'il est technologiquement possible d'appliquer le concept d'AI lors d'une attaque, il existe certains défis, tels que la complexité du système de menaces, la nécessité de faire appel au renseignement, et l'utilisation de différents types de pare-feu et de mots de passe (Yasar, Yasar, et Topcu 2012).

Internet des objets militaires (IoMT)

L'Internet des objets militaires (IoMT) est un réseau complexe d'entités interconnectées, ou « objets » aux avantages reconnus (Silicon Labs 2013), qui communiquent entre elles pour se coordonner, apprendre et interagir avec l'environnement pour un large éventail d'activités. de manière plus efficace et informée (Rowlands 2017) (Cameron 2018). L'idée de base est que les futures batailles militaires seront dominées par l'intelligence artificielle et la cyberguerre (Kott, Alberts, et Wang 2015).

Les objects (« things ») de l'IoMT possèdent des capacités physiques intelligentes pour détecter, apprendre et agir via des interfaces virtuelles ou cyber-interfaces intégrées (Kott 2018). En général, les objects IoMT forment une « structure de données » (Sydney J. Freedberg Jr 2020) pour le transport, la capture, la détection et l'actionnement des données, et un dispositif global doté de capacités de traitement et de communication qui peuvent échanger des informations avec le réseau plus vaste (Russell et Abdelzaher 2018). La possibilité d'incorporer des objets inanimés, tels que des plantes et des roches, dans le système en les équipant de capteurs qui les transformeront en points de collecte d'informations a également été suggérée (Parker 2018) (e-Plants(Saxena 2017)).

Table des matières

Livre



La guerre électronique est un élément essentiel des opérations militaires modernes et a connu des progrès significatifs ces dernières années. Ce livre donne un aperçu de la guerre électronique, de son évolution historique, de ses composants clés et de son rôle dans les scénarios de conflit contemporains. Il aborde également les tendances et les défis émergents en matière de guerre électronique et sa pertinence contemporaine à l'ère des technologies avancées et des cybermenaces, en soulignant la nécessité de poursuivre la recherche et le développement dans ce domaine.

Le livre explore l'intersection naissante de l'intelligence artificielle et de la guerre électronique, mettant en lumière l'évolution du paysage des conflits modernes et les implications de l'intégration des technologies avancées. Les rôles multiformes de l'intelligence artificielle dans la guerre électronique sont mis en évidence, en examinant ses avantages potentiels, les considérations éthiques et les défis associés à son intégration.

MultiMedia Publishing https://www.telework.ro/fr/e-books/la-guerre-electronique-et-lintelligence-artificielle/

Digital: EPUB (ISBN 978-606-033-863-5), Kindle (ISBN 978-606-033-864-2) PDF (ISBN 978-606-033-865-9)

DOI: 10.58679/MM37958

Date de publication: 11.07.2024

Bibliographie

* * *. 1984. *Voennyi Entsiklopedicheskii Slovar*. Moscova: Voennoe Izadatelstvo.

———. 1990. *Voenno-morskoi Slovar*. Moscova: Voennoe Izadatelstvo.

———. 2000. « Electronic Warfare Fundamentals ». https://falcon.blu3wolf.com/Docs/Electronic-Warfare-Fundamentals.pdf.

Adams, Charlotte. 2018. « Cognitive Electronic Warfare: Radio Frequency Spectrum Meets Machine Learning ». 2018. //interactive.aviationtoday.com/avionicsmagazine/august-september-2018/cognitive-electronic-warfare-radio-frequency-spectrum-meets-machine-learning/.

Adamy, David. 2001. *EW 101: A First Course in Electronic Warfare*. Artech House.

AIM. 2019. « The AIM Initiative: A Strategy for Augmenting Intelligence Using Machines ». 2019. https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2019/3286-the-aim-initiative-a-strategy-for-augmenting-intelligence-using-machines.

Akhtar, Jabran, et Karl Erik Olsen. 2018. « A Neural Network Target Detector with Partial CA-CFAR Supervised Training ». In *2018 International Conference on Radar (RADAR)*, 1-6. https://doi.org/10.1109/RADAR.2018.8557276.

Allen, Gregory C. 2019. *Understanding China's AI Strategy: Clues to Chinese Strategic Thinking on Artificial Intelligence and National Security*. Center for a New American Security.

Allen, John, et Giampiero Massolo. 2020. *The Global Race for Technological Superiority. Discover the Security Implication*. Édité par Fabio Rugge. Milan: Ledizioni.

Amuru, SaiDhiraj, Cem Tekin, Mihaela van der Schaar, et R. Michael Buehrer. 2015. « A systematic learning method for optimal jamming ». In *2015 IEEE International Conference on Communications (ICC)*, 2822-27. https://doi.org/10.1109/ICC.2015.7248754.

Army, United States Government US. 1996. « Joint Pub 3-58 Joint Doctrine for Military Deception ».

https://webharvest.gov/peth04/20041021042923/http://www.dtic.mil/doctrine/jel/new_pubs/jp3_58.pdf.

———. 2000. « Joint Publication 3-51 Joint Doctrine for Electronic Warfare ». https://irp.fas.org/doddir/dod/jp3_51.pdf.

———. 2016. « Joint Publication JP 1-02 Department of Defense Dictionary of Military and Associated Terms ». https://irp.fas.org/doddir/dod/jp1_02.pdf.

———. 2020a. *Joint Publication JP 3-13 Information Operations Change 1 November 2014*. Independently Published.

———. 2020b. « Joint Vision 2020: America's Military - Preparing for Tomorrow ». https://apps.dtic.mil/sti/citations/ADA526044.

Baker, James E. 2018. « Artificial intelligence and national security law: A dangerous nonchalance | MIT Center for International Studies ». 2018. https://cis.mit.edu/publications/starr-forum-report/18-01-report.

Barshan, Billur, et Bahaeddin Eravci. 2012. « Automatic Radar Antenna Scan Type Recognition in Electronic Warfare ». *IEEE Transactions on Aerospace and Electronic Systems* 48 (4): 2908-31. https://doi.org/10.1109/TAES.2012.6324669.

Bronk, Justin, Nick Reynolds, et Jack Watling. 2022. « The Russian Air War and Ukrainian Requirements for Air Defence ». https://static.rusi.org/SR-Russian-Air-War-Ukraine-web-final.pdf.

Brooks, Risa. 2018. « Technology and Future War Will Test U.S. Civil-Military Relations ». War on the Rocks. 26 novembre 2018. https://warontherocks.com/2018/11/technology-and-future-war-will-test-u-s-civil-military-relations/.

Browne, J. P. R., et Michael T. Thurbon. 1998. *Electronic Warfare*. Brassey's.

Browne, Jack. 2017. « Cognitive EW Provides Computer-Powered Protection ». Microwaves & RF. 10 mai 2017. https://www.mwrf.com/markets/defense/article/21848321/cognitive-ew-provides-computerpowered-protection.

Brunt, Leroy B. Van. 1978. *Applied ECM*. EW Engineering.

BSI. 2023. « Federal Office for Information Security ». Federal Office for Information Security. 6 novembre 2023. https://www.bsi.bund.de/EN/Home/home_node.html.

Butt, Faran, et Madiha Jalil. 2013. *An overview of electronic warfare in radar systems*. https://doi.org/10.1109/TAEECE.2013.6557273.

Cameron, Lori. 2018. « Internet of Things Meets the Military and Battlefield: Connecting Gear and Biometric Wearables for an IoMT and IoBT ». IEEE Computer Society. 1 mars 2018. https://www.computer.org/publications/tech-news/research/internet-of-military-battlefield-things-iomt-iobt/.

Campen, Alan D. 1992. *The First Information War: The Story of Communications, Computers, and Intelligence Systems in the Persian Gulf War*. AFCEA International Press.

Carlin, John P. 2016. « Detect, Disrupt, Deter: A Whole-of-Government Approach to National Security Cyber Threats | CSIS Events ». 2016. https://www.csis.org/events/detect-disrupt-deter-whole-government-approach-national-security-cyber-threats.

Casterline, Kyle A., Nicholas J. Watkins, Jon R. Ward, William Li, et Matthew J. Thommana. 2022. « Applications of Machine Learning for Electronic Warfare Emitter Identification and Resource Management ». https://secwww.jhuapl.edu/techdigest/content/techdigest/pdf/V36-N02/36-02-Casterline.pdf.

Chen, Jian, Shiyou Xu, Jiangwei Zou, et Zengping Chen. 2019. « Interrupted-Sampling Repeater Jamming Suppression Based on Stacked Bidirectional Gated Recurrent Unit Network and Infinite Training ». *IEEE Access* 7:107428-37. https://doi.org/10.1109/ACCESS.2019.2932793.

Clark, Colin. 2018. « Russia Widens EW War, "Disabling" EC-130s OR AC-130s In Syria ». *Breaking Defense* (blog). 24 avril 2018. https://breakingdefense.sites.breakingmedia.com/2018/04/russia-widens-ew-war-disabling-ec-130s-in-syria/.

Coats, Daniel. 2021. « Intelligence Community Information Environment (IC IE) - Data Strategy ». https://www.dni.gov/files/documents/CIO/Data-Strategy_2017-2021_Final.pdf.

Congressional Research Service. 2020. « Artificial Intelligence and National Security (R45178) ». 2020. https://crsreports.congress.gov/product/details?prodcode=R45178.

Copp, Tara. 2021. « 'It Failed Miserably': After Wargaming Loss, Joint Chiefs Are Overhauling How the US Military Will Fight ». Defense One. 26 juillet 2021. https://www.defenseone.com/policy/2021/07/it-failed-miserably-after-wargaming-loss-joint-chiefs-are-overhauling-how-us-military-will-fight/184050/.

CRA. 2017. « Internet of Battlefield Things (IoBT) CRA – DEVCOM Army Research Laboratory ». 2017. https://arl.devcom.army.mil/cras/iobt-cra/.

CRS. 2022. « Defense Primer: Electronic Warfare ». https://sgp.fas.org/crs/natsec/IF11118.pdf.

CS Europe. 2023. « Cyber Security Europe | Cyber Security Insight for Boardroom and C-Suite Executives. » Cyber Security Europe. 2023. https://www.cseurope.info/.

Davenport, Thomas, et Ravi Kalakota. 2019. « The Potential for Artificial Intelligence in Healthcare ». *Future Healthc J* 6 (2): 94-98. https://doi.org/10.7861/futurehosp.6-2-94.

Davis, Zachary. 2019. « Artificial Intelligence on the Battlefield: Implications for Deterrence and Surprise ». *PRISM* 8 (2): 114-31.

Day, Peter. 2016. « Peter Day's World of Business Podcast ». 2016. http://downloads.bbc.co.uk/podcasts/radio/worldbiz/worldbiz_20150319-0730a.mp3.

De Spiegeleire, Stephan, Matthijs Maas, et Tim Sweijs. 2017. *Artificial Intelligence and the Future of Defense*.

Department of Defense. 2018. « Summary of the 2018 National Defense Strategy ». https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

Dickson, John R. V. 1987. « Electronic Warfare in Vietnam: Did We Learn Our Lessons?. » In . https://www.semanticscholar.org/paper/Electronic-Warfare-in-Vietnam%3A-Did-We-Learn-Our-Dickson/399e7323fb081cb95db35d3a9d3075154a0de068.

DOD. 2020. « DoD Data Strategy ». https://media.defense.gov/2020/Oct/08/2002514180/-1/-1/0/DOD-DATA-STRATEGY.PDF.

DoD. 2022. « DoD Announces Release of JADC2 Implementation Plan ». U.S. Department of Defense. 2022. https://www.defense.gov/News/Releases/Release/Article/2970094/dod-announces-release-of-jadc2-implementation-plan/https%3A%2F%2Fwww.defense.gov%2FNews%2FReleases%2FRelease%2FArticle%2F2970094%2Fdod-announces-release-of-jadc2-implementation-plan%2F.

Doskalov, Mikhail. 2013. « Perspektivy razvitiia sistemy radioelektronnoi borby Rossiiskoj Federatsii na period do 2020 goda ». In *Oboronnyi kompleks RF: Sostoianie i razvitie*. http://federalbook.ru/files/OPK/Soderjanie/OPK-9/III/Doskalov.pdf.

Dudczyk, Janusz, et A. Kawalec. 2013. « Specific emitter Identification based on graphical representation of the distribution of radar signal parameters ». *Jokull* 63 (novembre):408-16.

Duke, Audrey. 2023. « Harnessing Chaos: Unleashing Electromagnetic Warfare for Enhanced Joint Operations ». https://apps.dtic.mil/sti/citations/AD1206172.

Dunn Cavelty, Myriam. 2012. « Cyber-Allies: Strengths and Weaknesses of NATO's Cyberdefense Posture ». SSRN Scholarly Paper. Rochester, NY. https://papers.ssrn.com/abstract=1997153.

EASA. 2020. « Concepts of Design Assurance for Neural Networks (CoDANN) ». https://www.easa.europa.eu/sites/default/files/dfu/EASA-DDLN-Concepts-of-Design-Assurance-for-Neural-Networks-CoDANN.pdf.

Elbir, Ahmet M., Kumar Vijay Mishra, et Yonina C. Eldar. 2019. « Cognitive Radar Antenna Selection via Deep Learning ». arXiv. https://doi.org/10.48550/arXiv.1802.09736.

EMK, SU. 2023. « ECHO Network ». 2023. https://echonetwork.eu/.

European Defence Agency. 2023. « Enhancing EU Military Capabilities Beyond 2040 ». https://eda.europa.eu/docs/default-source/eda-publications/enhancing-eu-military-capabilities-beyond-2040.pdf.

Freedberg, Sydney J. 2014. « US Has Lost "Dominance In Electromagnetic Spectrum": Shaffer ». *Breaking Defense* (blog). 3 septembre 2014. https://breakingdefense.com/2014/09/us-has-lost-dominance-in-electromagnetic-spectrum-shaffer/.

———. 2017. « Electronic Warfare "Growing"; Joint Airborne EW Study Underway ». *Breaking Defense* (blog). 23 juin 2017. https://breakingdefense.sites.breakingmedia.com/2017/06/electronic-warfare-growing-joint-airborne-ew-study-underway/.

Friedrich, Nancy. 2020. « AI and Machine Learning Redefine the EW Landscape | 2020-12-08 | Microwave Journal ». 2020. https://www.microwavejournal.com/articles/35107-ai-and-machine-learning-redefine-the-ew-landscape.

Fulghum, David A., et Robert Wall. 2007. « Israel Shows Electronic Prowess | Aviation Week Network ». 2007. https://aviationweek.com/israel-shows-electronic-prowess.

Gambrell, Dorothy, et Charissa Isidro. 2022. « A Visual Guide to the World's Military Budgets ». *Bloomberg.Com*, 11 mars 2022. https://www.bloomberg.com/news/features/2022-03-11/the-largest-militaries-visualized.

Gannon, Brian P. 2023. « Implement AI in Electromagnetic Spectrum Operations ». U.S. Naval Institute. 1 août 2023. https://www.usni.org/magazines/proceedings/2023/august/implement-ai-electromagnetic-spectrum-operations.

Gao, Jingpeng, Yi Lu, Junwei Qi, et Liangxi Shen. 2019. « A Radar Signal Recognition System Based on Non-Negative Matrix Factorization Network and Improved Artificial Bee Colony Algorithm ». *IEEE Access* 7:117612-26. https://doi.org/10.1109/ACCESS.2019.2936669.

Gecgel Cetin, Selen, Caner Goztepe, et Gunes Karabulut Kurt. 2019. *Jammer Detection based on Artificial Neural Networks: A Measurement Study*. https://doi.org/10.1145/3324921.3328788.

Gigova, Radina. 2017. « Who Putin thinks will rule the world | CNN ». 2017. https://edition.cnn.com/2017/09/01/world/putin-artificial-intelligence-will-rule-world/index.html.

Goodfellow, Ian, Yoshua Bengio, et Aaron Courville. 2016. *Deep Learning: Adaptive Computation and Machine Learning Series*. MIT Press.

Grant, P. M., et J. H. Collins. 1982. « Introduction to Electronic Warfare ». *IEE Proceedings F (Communications, Radar and Signal Processing)* 129 (3): 113-32. https://doi.org/10.1049/ip-f-1.1982.0020.

Gulhane, Tejaswi Singh and Amit. 2018. « 8 Key Military Applications for Artificial Intelligence ». 2018. https://blog.marketresearch.com/8-key-military-applications-for-artificial-intelligence-in-2018.

Guzenko, V. F., et A. L. Moraresku. 2017. *Radioelektronnaia borba. Sovremennoe soderzhanie*. Moscova: Informatsionnyi Most.

Haigh, Karen Zita, et Julia Andrusenko. 2021. *Cognitive Electronic Warfare: An Artificial Intelligence Approach*. Artech House.

Hamilton, Serena, A.J. Jakeman, et John Norton. 2008. « Artificial Intelligence techniques: An introduction to their use for modelling environmental systems ». *Mathematics and Computers in Simulation* 78 (juillet):379-400. https://doi.org/10.1016/j.matcom.2008.01.028.

Haney, Brian. 2019. « Applied Artificial Intelligence in Modern Warfare and National Security Policy ». SSRN Scholarly Paper. Rochester, NY. https://doi.org/10.2139/ssrn.3454204.

Henney, Megan. 2019. « Big Tech Has Spent $582M Lobbying Congress. Here's Where That Money Went ». Text.Article. FOXBusiness. Fox Business. 8 mai 2019. https://www.foxbusiness.com/technology/amazon-apple-facebook-google-microsoft-lobbying-congress.

Hoehn, John. 2021. « Defense Primer: What Is Command and Control? » https://apps.dtic.mil/sti/citations/AD1169627.

Insinna, Valerie. 2022. « China Could Obtain 1,500 Nuclear Warheads by 2035, Pentagon Estimates ». *Breaking Defense* (blog). 29 novembre 2022. https://breakingdefense.sites.breakingmedia.com/2022/11/china-to-obtain-1500-nuclear-warheads-by-2035-pentagon-estimates/.

Jankowicz, Mia. 2023. « Ukraine Is Losing 10,000 Drones a Month to Russian Electronic-Warfare Systems That Send Fake Signals and Screw with Their Navigation, Researchers Say ». Business Insider. 2023. https://www.businessinsider.com/ukraine-losing-10000-drones-month-russia-electronic-warfare-rusi-report-2023-5.

Judd, Denis, et Keith Surridge. 2013. *The Boer War: A History*. Bloomsbury Academic.

Junfei, Yu, Li Jingwen, Sun Bing, et Jiang Yuming. 2018. « Barrage Jamming Detection and Classification Based on Convolutional Neural Network for Synthetic Aperture Radar ». In *IGARSS 2018 - 2018 IEEE International Geoscience and Remote Sensing Symposium*, 4583-86. https://doi.org/10.1109/IGARSS.2018.8519373.

Kadlecová, Lucie, Nadia Meyer, Rafaël Cos, et Pauline Ravinet. 2020. « Mapping the Role of Science Diplomacy in the Cyber Field ».

Kang, Li, Jiu Bo, Liu Hongwei, et Liang Siyuan. 2018. « Reinforcement Learning based Anti-jamming Frequency Hopping Strategies Design for Cognitive Radar ». In *2018 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC)*, 1-5. https://doi.org/10.1109/ICSPCC.2018.8567751.

Katz, Yaakov. 2010. « And They Struck Them with Blindness ». The Jerusalem Post | JPost.Com. 29 septembre 2010. https://www.jpost.com/magazine/features/and-they-struck-them-with-blindness.

Kjellén, Jonas. 2018. « Russian Electronic Warfare - The role of Electronic Warfare in the Russian Armed Forces ». https://web.archive.org/web/20181010174505/https://www.foi.se/report-search/pdf?fileName=D%3A%5CReportSearch%5CFiles%5C4c547bec-bdfa-4bdb-a1c9-018097aaf615.pdf.

Kolesov, N. A., et I. G. Nasenkov. 2015. *Radioelektronnaia Borba. Ot eksperimentov proshlogo do reshayushchego fronta budushchego*. Moscova: Centre for Analysis of Strategies and Technologies (CAST).

Kolhatkar, Sheelah. 2019. « How Elizabeth Warren Came Up with a Plan to Break Up Big Tech ». *The New Yorker*, 20 août 2019. https://www.newyorker.com/business/currency/how-elizabeth-warren-came-up-with-a-plan-to-break-up-big-tech.

Kott, Alexander. 2018. « Challenges and Characteristics of Intelligent Autonomy for Internet of Battle Things in Highly Adversarial Environments », mars.

Kott, Alexander, David S. Alberts, et Cliff Wang. 2015. « Will Cybersecurity Dictate the Outcome of Future Wars? » *Computer* 48 (12): 98-101. https://doi.org/10.1109/MC.2015.359.

Krylov, G. O., S. L. Larionova, et Nikitina. 2017. *Bazovye poniatiia informatsionnoi bezopasnosti*. Moscova: OOO RUSAJNS.

Kube, Courtney. 2018. « Russia Is Jamming American Drones in Syria, Officials Say ». NBC News. 10 avril 2018. https://www.nbcnews.com/news/military/russia-has-figured-out-how-jam-u-s-drones-syria-n863931.

Kucukozyigit, Ali. 2006. « Electronic Warfare (EW) Historical Perspectives and Its Relationship to Information Operations (IO) - Considerations for Turkey ».

Lakhin, Andrei, et Andrei Korobeinikov. 2016. *Sostoianie i perspektivy razvitiia voisk radioelektronnoi borby Vooruzhennykh Sil Rossiiskoi Federatsii*. Moscova: Informatsionnyi Most.

Lazarov, Lazar. 2019. « Perspectives and Trends for the Development of Electronic Warfare Systems ». *2019 International Conference on Creative Business for Smart and Sustainable Growth (CREBUS)*, mars, 1-3. https://doi.org/10.1109/CREBUS.2019.8840074.

Lee, Gyeong-Hoon, Jeil Jo, et Cheong Hee Park. 2020. « Jamming Prediction for Radar Signals Using Machine Learning Methods ». *Security and Communication Networks* 2020 (janvier):e2151570. https://doi.org/10.1155/2020/2151570.

Li, Huiqin, Yanling Li, Chuan He, Jianwei Zhan, et Hui Zhang. 2021. « Cognitive Electronic Jamming Decision-Making Method Based on Improved Q -Learning Algorithm ». *International Journal of Aerospace Engineering* 2021 (décembre):1-12. https://doi.org/10.1155/2021/8647386.

Li, Xueqiong, Zhitao Huang, Fenghua Wang, Xiang Wanga, et Tianrui Liu. 2018. « Toward Convolutional Neural Networks on Pulse Repetition Interval Modulation Recognition ». *IEEE Communications Letters* PP (août):1-1. https://doi.org/10.1109/LCOMM.2018.2864725.

Li, Yangyang, Ximing Wang, Dianxiong Liu, Qiuju Guo, Xin Liu, Jie Zhang, et Yitao Xu. 2019. « On the Performance of Deep Reinforcement Learning-Based Anti-Jamming Method Confronting Intelligent Jammer ». *Applied Sciences* 9 (7): 1361. https://doi.org/10.3390/app9071361.

Liao, Xiaofeng, Bo Li, et Bo Yang. 2018. « A Novel Classification and Identification Scheme of Emitter Signals Based on Ward’s Clustering and Probabilistic Neural Networks with Correlation Analysis ». *Computational Intelligence and Neuroscience* 2018 (novembre):e1458962. https://doi.org/10.1155/2018/1458962.

Liu, Yemin, Shiqi Xing, Y. Li, Dong Hou, et Wang Xuesong. 2017. « Jamming recognition method based on the polarization scattering characteristics of chaff clouds ». *IET Radar, Sonar & Navigation* 11 (août). https://doi.org/10.1049/iet-rsn.2017.0121.

Liubin, Mikhail Dmitriyevich. 2009. « K voprosu ob istorii razvitiia i perspektivakh radioelektronnoi borby ». *Voennaia mysl*, nº 3, 64-75.

Magrassi, Paolo. 2002a. *A World of Smart Objects: The Role of Auto-Identification Technologies*.

———. 2002b. *Why a Universal RFID Infrastructure Would Be a Good Thing*.

MarketsAndMarkets. 2023. « Artificial Intelligence (AI) in Military Market Size Growth Opportunities Industry Trends and Analysis 2030 ». MarketsandMarkets. 2023. https://www.marketsandmarkets.com/Market-Reports/artificial-intelligence-military-market-41793495.html.

Martino, Andrea De. 2012. *Introduction to Modern EW Systems*. Artech House.

McArthur, Charles W. 1990. *Operations Analysis in the United States Army Eighth Air Force in World War II*. American Mathematical Soc.

McDermott, Roger N. 2017. « Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum ». ICDS. 17 septembre 2017. https://icds.ee/en/russias-electronic-warfare-capabilities-to-2025-challenging-nato-in-the-electromagnetic-spectrum/.

MeriTalk. 2018. « DARPA Floats a Proposal for the Ocean of Things ». 2018. https://www.meritalk.com/articles/darpa-floats-a-proposal-for-the-ocean-of-things/.

Microwaves, Microwaves & RF. 2019. « BAE Bets on Use of Artificial Intelligence in Electronic Warfare ». Microwaves & RF. 15 juillet 2019. https://www.mwrf.com/markets/defense/article/21849838/bae-systems-bae-bets-on-use-of-artificial-intelligence-in-electronic-warfare.

Ministry of Defence. 2021a. « Data Strategy for Defence ». GOV.UK. 2021. https://www.gov.uk/government/publications/data-strategy-for-defence.

———. 2021b. « Digital Strategy for Defence ». GOV.UK. 2021. https://www.gov.uk/government/publications/digital-strategy-for-defence-delivering-the-digital-backbone-and-unleashing-the-power-of-defences-data.

———. 2022. « Defence Artificial Intelligence Strategy ». GOV.UK. 2022. https://www.gov.uk/government/publications/defence-artificial-intelligence-strategy/defence-artificial-intelligence-strategy.

Mizokami, Kyle. 2023. « Why Ukraine's GPS-Guided Bombs Keep Missing Their Targets ». Popular Mechanics. 20 avril 2023. https://www.popularmechanics.com/military/weapons/a43591694/russian-jamming-gps-guided-bombs/.

NATO. 2019. « The 107th NATO Electronic Warfare Advisory Committee (NEWAC) Convenes in Brussels ». NATO. 2019. https://www.nato.int/cps/en/natohq/news_171280.htm.

———. 2023. « Electromagnetic Warfare ». NATO. 2023. https://www.nato.int/cps/en/natohq/topics_80906.htm.

Neri, F. 1991. « Introduction to electronic defense systems ». In . https://www.semanticscholar.org/paper/Introduction-to-electronic-defense-systems-Neri/8d8aed6d92ecf7af850f09a2ee740380c2d4b366.

Noh, Sanguk, et Unseob Jeong. 2010. « Intelligent Command and Control Agent in Electronic Warfare Settings ». *International Journal of Intelligent Systems* 25 (6): 514-28. https://doi.org/10.1002/int.20413.

Northrop. 2022. « Electronic Warfare and Sensors ». https://info.breakingdefense.com/hubfs/E-Book_EW_&_Sensors_Northrop_Grumman_Breaking_Defense.pdf.

ODIN. 2023. « Borisoglebsk-2 (RB-301B) Russian Amphibious Multipurpose Jamming Complex ». 2023. https://odin.tradoc.army.mil/WEG/Asset/Borisoglebsk-2_(RB-301B)_Russian_Amphibious_Multipurpose_Jamming_Complex.

Parker, Paul. 2018. « The Internet of Battlefield Things Is Coming. Are IT Pros Ready? » C4ISRNet. 3 octobre 2018. https://www.c4isrnet.com/opinion/2018/10/03/the-internet-of-battlefield-things-is-coming-are-it-pros-ready/.

Petrov, Nedyalko, Ivan Jordanov, et Jon Roe. 2013. « Radar Emitter Signals Recognition and Classification with Feedforward Networks ». *Procedia Computer Science*, 17th International Conference in Knowledge Based and Intelligent Information and Engineering Systems - KES2013, 22 (janvier):1192-1200. https://doi.org/10.1016/j.procs.2013.09.206.

Poisel, Richard. 2008. *Introduction to Communication Electronic Warfare Systems*. Artech House.

Polit, Kate. 2018. « Army Takes on Wicked Problems With the Internet of Battlefield Things ». 2018. https://www.meritalk.com/articles/army-takes-on-wicked-problems-with-the-internet-of-battlefield-things/.

Polmar, Norman. 1979. « The U. S. Navy: Electronic Warfare (Part 2) ». U.S. Naval Institute. 1 novembre 1979. https://www.usni.org/magazines/proceedings/1979/november/u-s-navy-electronic-warfare-part-2.

Price, Alfred. 1984. *The History of US Electronic Warfare*. Association of Old Crows.

Qiang, Xing, Zhu Wei-gang, et Bo Yuan. 2018. « Jamming Style Selection for Small Sample Radar Jamming Rule Base ». *2018 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC)*, septembre, 1-5. https://doi.org/10.1109/ICSPCC.2018.8567613.

Qu, Zhiyu, Wenyang Wang, Changbo Hou, et Chenfan Hou. 2019. « Radar Signal Intra-Pulse Modulation Recognition Based on Convolutional Denoising Autoencoder and Deep Convolutional Neural Network ». *IEEE Access* 7:112339-47. https://doi.org/10.1109/ACCESS.2019.2935247.

Rahman, H. 2019. *Introduction to Electronic Defense Systems*. Boca Raton, FL, USA: CRC Press.

Rambo. 2009. « Information Warfare: History of Electronic Warfare ». *INFORMATION WARFARE* (blog). 7 décembre 2009. https://ew30.blogspot.com/2009/12/such-is-reliance-on-electromagnetic-em.html.

Rogosa, Alexander. 2015. « Shifting Spaces: The Success of the SpaceX Lawsuit and the Danger of Single-Source Contracts in America's Space Program ». *Federal Circuit Bar Journal* 25:101.

Rowlands, Greg. 2017. « The Internet of Military Things & Machine Intelligence: A Winning Edge or Security Nightmare? | Australian Army Research Centre (AARC) ». 2017. https://researchcentre.army.gov.au/library/land-power-forum/internet-military-things-machine-intelligence-winning-edge-or-security-nightmare.

Russell, Stephen, et Tarek Abdelzaher. 2018. « The Internet of Battlefield Things: The Next Generation of Command, Control, Communications and Intelligence (C3I) Decision-Making ». In *MILCOM 2018 - 2018 IEEE Military Communications Conference (MILCOM)*, 737-42. https://doi.org/10.1109/MILCOM.2018.8599853.

Saxena, Shalini. 2017. « Researchers Create Electronic Rose Complete with Wires and Supercapacitors ». Ars Technica. 1 mars 2017.

https://arstechnica.com/science/2017/03/researchers-grow-electronic-rose-complete-with-wires-and-supercapacitors/.

Sfetcu, Nicolae. 2023a. « Evoluția inteligenței artificiale în domeniul securității naționale ». Intelligence Info. 10 novembre 2023. https://www.intelligenceinfo.org/evolutia-inteligentei-artificiale-in-domeniul-securitatii-nationale/.

———. 2023b. « Rolul serviciilor de informații în război ». Intelligence Info. 3 août 2023. https://www.intelligenceinfo.org/rolul-serviciilor-de-informatii-in-razboi/.

———. 2024. « Războiul electronic și inteligența artificială ». MultiMedia. 8 janvier 2024. https://www.telework.ro/ro/e-books/razboiul-electronic-si-inteligenta-artificiala/.

Shankar, M., et B. Mohan. 2013. « Recent Advances in Electronic Warfare-ESM Systems ». In . https://www.semanticscholar.org/paper/RECENT-ADVANCES-IN-ELECTRONIC-WARFARE-ESM-SYSTEMS-Shankar-Mohan/bf6e4c372514695dd167eebf6f9dfb78ca120f6a.

Shao, Guangqing, Yushi Chen, et Yinsheng Wei. 2020. « Convolutional Neural Network-Based Radar Jamming Signal Classification With Sufficient and Limited Samples ». *IEEE Access* 8:80588-98. https://doi.org/10.1109/ACCESS.2020.2990629.

Sharma, Purabi, Kandarpa Kumar Sarma, et Nikos E. Mastorakis. 2020. « Artificial Intelligence Aided Electronic Warfare Systems- Recent Trends and Evolving Applications ». *IEEE Access* 8:224761-80. https://doi.org/10.1109/ACCESS.2020.3044453.

Silicon Labs. 2013. « The Evolution of Wireless Sensor Networks ». https://www.silabs.com/documents/public/white-papers/evolution-of-wireless-sensor-networks.pdf.

Simonite, Tom. 2017. « Artificial Intelligence Fuels New Global Arms Race ». *Wired*, 2017. https://www.wired.com/story/for-superpowers-artificial-intelligence-fuels-new-global-arms-race/.

Singer, Peter W., et Allan Friedman. 2014. *Cybersecurity: What Everyone Needs to Know*. OUP USA.

Singh, Mohinder. 1988. « Electronic Warfare ». https://www.drdo.gov.in/sites/default/files/publcations-document/Electronic%20Warfare.pdf.

Skolnik, Merrill I. 2008. *Radar Handbook, Third Edition*. McGraw-Hill Education.

Smith, Craig. 2019. « Eye On AI ». Eye On AI. 28 août 2019. https://www.eye-on.ai.

Smith, Patrick. 2022. *Russian Electronic Warfare: A Growing Threat to U.S. Battlefield Supremacy*. American Security Project.

Smith, Ron, et Scott Knight. 2005. « Applying Electronic Warfare Solutions to Network Security - Canadian Military Journal ». 2005. http://www.journal.forces.gc.ca/vo6/no3/electron-eng.asp.

SPARTA. 2023. « SPARTA Consortium ». 2023. https://www.cybersecurityintelligence.com/sparta-consortium-5594.html.

Stackpole, Beth. 2016. « Keeping the Connected Soldier Connected with Simulation ». Digital Engineering. 1 septembre 2016. https://www.digitalengineering247.com/article/keeping-the-connected-soldier-connected-with-simulation.

State Council. 2017. « A Next Generation Artificial Intelligence Development Plan ». *China Copyright and Media* (blog). 20 juillet 2017. https://chinacopyrightandmedia.wordpress.com/2017/07/20/a-next-generation-artificial-intelligence-development-plan/.

Sydney J. Freedberg Jr. 2020. « Project Rainmaker: Army Weaves 'Data Fabric' To Link Joint Networks ». *Breaking Defense* (blog). 17 novembre 2020. https://breakingdefense.sites.breakingmedia.com/2020/11/project-rainmaker-army-weaves-data-fabric-to-link-joint-networks/.

Taddeo, Mariarosaria. 2012. « An analysis for a just cyber warfare ». In *2012 4th International Conference on Cyber Conflict (CYCON 2012)*, 1-10. https://ieeexplore.ieee.org/document/6243976.

Tang, Author: Hazel. 2020. « Preparing for the Future of Artificial Intelligence. Executive Office of the President: National Science and Technology Council and Committee on Technology. October, 2016. » *AIMed* (blog). 9 avril 2020. https://ai-med.io/executive/preparing-for-the-future-of-artificial-intelligence-executive-office-of-the-president-national-science-and-technology-council-and-committee-on-technology-october-2016/.

Tegler, Eric. 2022. « The Vulnerability of AI Systems May Explain Why Russia Isn't Using Them Extensively in Ukraine ». Forbes. 2022. https://www.forbes.com/sites/erictegler/2022/03/16/the-vulnerability-of-artificial-intelligence-systems-may-explain-why-they-havent-been-used-extensively-in-ukraine/.

Tegmark, Max. 2018. « Life 3.0: Being Human in the Age of Artificial Intelligence | Mitpressbookstore ». 31 juillet 2018. https://mitpressbookstore.mit.edu/book/9781101970317.

Tsui, Chi-Hao Cheng, James. 2022. *An Introduction to Electronic Warfare; from the First Jamming to Machine Learning Techniques*. New York: River Publishers. https://doi.org/10.1201/9781003337171.

Tucker, Patrick. 2022. « AI Is Already Learning from Russia's War in Ukraine, DOD Says ». Defense One. 21 avril 2022. https://www.defenseone.com/technology/2022/04/ai-already-learning-russias-war-ukraine-dod-says/365978/.

US Marine Corps. 2016. « Electronic Warfare ». https://www.marines.mil/Portals/1/Publications/MCRP%203-32D.1%20(Formerly%20MCWP%203-40.5).pdf.

Vincent, James. 2017. « Elon Musk and AI Leaders Call for a Ban on Killer Robots ». The Verge. 21 août 2017. https://www.theverge.com/2017/8/21/16177828/killer-robots-ban-elon-musk-un-petition.

Waghray, Namrita, et P. M. Menghal. 2011. « Simulation of radar topology networks to evolve the electronic warfare survivability metrics ». *2011 3rd International Conference on Electronics Computer Technology*, avril, 355-59. https://doi.org/10.1109/ICECTECH.2011.5941622.

Wan, Tao, Xinying Fu, Kaili Jiang, Yuan Zhao, et Bin Tang. 2019. « Radar Antenna Scan Pattern Intelligent Recognition Using Visibility Graph ». *IEEE Access* 7:175628-41. https://doi.org/10.1109/ACCESS.2019.2957769.

Wang, Feng, Shanshan Huang, Hao Wang, et Chenlu Yang. 2018. « Automatic Modulation Classification Exploiting Hybrid Machine Learning Network ». *Mathematical Problems in Engineering* 2018 (décembre):e6152010. https://doi.org/10.1155/2018/6152010.

Wei, Dongxu, Shuning Zhang, Si Chen, Huichang Zhao, et Linzhi Zhu. 2019. « Research on Deception Jamming of Chaotic Composite Short-Range Detection System Based on Bispectral Analysis and Genetic Algorithm–Back Propagation ». *International Journal of Distributed Sensor Networks* 15 (5): 1550147719847444. https://doi.org/10.1177/1550147719847444.

Weisgerber, Marcus. 2017. « The Pentagon's New Algorithmic Warfare Cell Gets Its First Mission: Hunt ISIS ». Defense One. 14 mai 2017. https://www.defenseone.com/technology/2017/05/pentagons-new-algorithmic-warfare-cell-gets-its-first-mission-hunt-isis/137833/.

Yasar, Nurgul, Fatih Mustafa Yasar, et Yucel Topcu. 2012. « Operational advantages of using Cyber Electronic Warfare (CEW) in the battlefield ». In *Cyber Sensing 2012*, 8408:151-59. SPIE. https://doi.org/10.1117/12.919454.

You, Shixun, Ming Diao, et Lipeng Gao. 2019. « Deep Reinforcement Learning for Target Searching in Cognitive Electronic Warfare ». *IEEE Access* 7:37432-47. https://doi.org/10.1109/ACCESS.2019.2905649.

Zhang, Ming, Ming Diao, Lipeng Gao, et Lutao Liu. 2017. « Neural Networks for Radar Waveform Recognition ». *Symmetry* 9 (5): 75. https://doi.org/10.3390/sym9050075.